Atti Accademia Peloritana dei Pericolanti
Classe I di Scienze Fis. Mat. e Nat.
Vol. LXXIII (1995) - Adunanza del 20 ottobre 1995

INTEGRABLE DERIVATIONS III

H. MATSUMURA - G. RESTUCCIA

Abstract

We establish some theorems of structure for a ring A I-adically complete, I ideal of A, modulo the strong integrability of a finite number of derivations of A, in the case of the unequal characteristic.

Riassunto

Si stabiliscono teoremi di struttura per un anello A I-adicamente completo, I ideale dell'anello, modulo l'integrabilità forte di un numero finito di derivazioni di A, nel caso della caratteristica diseguale.

Introduction.

In this paper we will investigate the integrability of derivations in rings of unequal characteristic.

This case was examined in [2], but it is very important derive some theorems of strong integrability for derivations in analogue manner that for a k-algebra A, k field of characteristic $p > 0$.

Let A be a ring and p be a prime number. If we assume that p is neither zero nor unit in A and that all prime numbers other than p are units in A, then we say that A is a ring of unequal characteristic.

The most important example is the case when A is a local ring of characteristic zero with residue field of characteristic p.

The unequal characteristic case is more complicated that the case of characteristic $p > 0$, but the important result obtained in [2], which say that any derivation of A into pA is strongly integrable, is the key to generalize the theorems contained in [3], to the case of a finite number of derivations of A into pA. These derivations are essentially different that those considered in [1], [3], because they apply the maximal ideal of A in itself, supposed A local.

In this work, all rings are assumed to be commutative with a unit element.

A local ring is a noetherian local ring.

Let A be a ring. The set of all derivations of A into itself is denoted by $\mathrm{Der}(A)$.

DEFINITION 1. *A differentiation* $\mathbf{D}$ *of* A *is a sequence* $\mathbf{D} = \{D_0 = 1, D_1, D_2, \dots\}$ *of additive endomorphisms* $D_i : A \to A$ *such that*

$$D_n(ab) = \sum_{i+j=n} D_i(a)D_j(b)$$

for any n.

The set of differentiations of A is denoted by $HS(A)$.

Let t be an indeterminate over A and put:

$$E(a) = \sum_{n=0}^{\infty} D_n(a)t^n \in A[[t]].$$

Then E is a ring homomorphism of A into $A[[t]]$ such that $a \equiv E(a) \bmod t$ for every $a \in A$, and conversely any such homomorphism E comes from a difefrentiation of A. We can identify E with $\mathbf{D}$.

If $\mathbf{D} = \{1, D_1, \ldots\}$ and $\mathbf{D}' = \{1, D_1', \ldots\}$ are differentiations of A,

$$\mathbf{D} \cdot \mathbf{D}' = \{1, D_1 + D_1', D_2 + D_1 D_1' + D_2', \ldots, \sum_{i=1}^{n} D_i D_{n-i}', \ldots\}$$

is again a differentiation of A.

DEFINITION 2. *A differentiation* $\mathbf{D}$ *is said to be iterative if:*

$$D_i \circ D_j = \binom{i+j}{i} D_{i+j} \quad \textit{for all} \quad i, j.$$

DEFINITION 3. *Two differentiations* $\mathbf{D} = \{1, D_1, \ldots\}$ *and* $\mathbf{D}' = \{1, D_1', \ldots\}$ *of* A *will be said to commute each other when* D_m *and* D_n' *commute for any* m, n.

If $\mathbf{D}$ and $\mathbf{D}'$ are iterative and commute each other, then their product $\mathbf{D} \cdot \mathbf{D}'$ is again iterative ([1], 1).

DEFINITION 4. *A derivation* $D \in Der(A)$ *is said to be integrable if there exists a differentiation* $\mathbf{D} = \{1, D_1, D_2, \ldots\}$ *of* A *with* $D_1 = D$.

If the ring A contains the rational number fied $\mathbf{Q}$, then every derivation $D \in \mathrm{Der}(A)$ can be uniquely prolonged to the iterative differentiation

$$\mathbf{D} = \{1, D, D^2/2!, D^3/3!, \ldots, D^n/n!, \ldots\}.$$

If A contains Z_{pZ}, p a prime number, p non zero-divisor of A, then every derivation $D : A \to pA$ can be prolonged to same iterative differentiation

$$\mathbf{D} = \{1, D, D^2/2!, D^3/3!, \ldots, D^n/n!, \ldots\}$$

since $\forall n \in N$, $D^n/n! \in A$ ([2], theorem 1), but every derivation is not always integrable in unequal characteristic ([2]) and in characteristic p ([1], [3]).

LEMMA 1. *Let A be a ring of unequal characteristic $p > 0$, $p \neq 2$. Assume that p is not a zero-divisor in A. Then the number* $N_k = \dfrac{p^{k-1}}{k+1} \in Z_{pZ}$, *for every integer* $k \geq 1$.

Proof. The total ring of quotients K of A contains Q and $N_k \in Q$. If $k = 1$, $N_1 = \dfrac{1}{2} \in Z_{pZ}$, since 2 is invertible in A.

Suppose $k > 1$. If $k+1$ is not a multiple of p, $k+1$ is invertible in A and we are done.

If $k+1$ is a multiple of p, since $p \neq 2$, $k+1 = p^t$ is verified if and only if $t \leq k-1$, hence the assertion.

THEOREM 1. *Let A be a notherian K-algebra, $K = Z_{pZ}$, and let x be a element of A such that $\cap x^n A = (0)$.*

Suppose that:

1) *p is not 0-divisor in A as well as in A/xA;*
2) *there exists a differentiation $E : A \to A[[t]]$ such that $E(x) = x + pt$.*

Then, if $z \in A$ and $xz \in F$, where $F = \{a \in A / E(a) = a\}$, we have $z = 0$ and x is not a 0-divisor in A.

Proof. Suppose that $xz = 0$, then

$$E(xz) = E(x)E(z) = (x + pt)(z + tD_1(z) + t^2 D_2(z) + \ldots) = 0,$$

$$xz + xD_1(z)t + xD_2(z)t^2 + \ldots + pzt + pD_1(z)t^2 + pD_2(z)t^3 + \ldots = 0.$$

$$\begin{cases} xD_1(z) + pz = 0 \\ xD_2 + pD_1(z) = 0 \\ \dots\dots\dots\dots\dots\dots \\ xD_{n+1}(z) + pD_n(z) = 0 \\ \dots\dots\dots\dots\dots\dots \end{cases}$$

Hence, $pz \in x^n A$, $\forall n > 0$, $pz = 0$ and $z = 0$, since p is not 0-divisor in A.

THEOREM 2. *Let A be a noetherian K-algebra, $K = Z_{pZ}$, and let x be an element of the Jacobson of A, Rad (A).*

Suppose that:

1) p is not 0-divisor in A as well in A/xA

2) there exists a derivation $D : A \to pA$ such that $D(x) = pu$, $u \in \cup(A)$ or:

2') there exists a differentiation such that $E(x) = x + pt$

Put $F = \{a \in A/D(a) = 0\}$ in case 2), $F = \{a \in A/E(a) = a\}$ in case 2') and $\Im = (x)$.

Then F is a subring of A and $F \cap \Im = (o)$.

Proof. In case 2), replacing D by a suitable linear combination, we may assume that $D(x) = p$.

Since and derivation $D : A \to pA$ is strongly integrable the iterative differentiation:

$$E(a) = \sum_0^\infty \frac{1}{n!} t^n D^n(a)$$

satisfies the condition 2. Thus is suffices consider case 2'). A is separated in the x-adic topology.

Consider $y \in \Im \cap F$, $y = xz$, $y \in F$.

Thus $D(y) = 0,\ E(y) = y$

$$E(xz) = xz = E(x)E(z) = (x + pt)(z + D_1(z)t + D_2(z)t^2 + \dots)$$

$$= xz + xD_1(z)t + \dots$$

One conclude in the in the same manner of theorem 1.

THEOREM 3. *Let A be a noetherian local K-algebra, $K = Z_{pZ}$, and let $x_1, x_2, \dots, x_r$ be elements of the Jacobson radical Rad (A) of A. Put $\Im = (x_1, x_2, \dots, x_r)$.*

Suppose:

1) *p is not 0-divisor in A as well in $A/(x_1, \dots, x_i)$ $1 \le i \le r$*
2) *ther exist $D^{(1)}, \dots, D^{(r)} : A \to pA$ such that $det(D^{(i)}(x_j)) = p^r u,\ u \in U(A)$;*

or:

2') *there exist differentiations $E^{(1)}, \dots, E^{(r)} : A \to A[[t]]$ such that $E^{(i)}(x_j) = x_j + pt\delta_{ij}$ $(i, j = 1, 2, \dots, r)$.*

Put $F = \{a \in /D^{(1)}(a) = \dots = D^{(r)}(a) = 0\}$ in case 2,
and $F = \{a \in /E^{(1)}(a) = \dots = E^{(r)}(a) = 0\}$ in case 2'.
Then F is a subring of A and $F \cap \Im = (0)$.

Proof. In case α, we can show that $D^{(i)}$, $i = 1, \dots, n$ are linearly independent over A.

Let be $\lambda_1 D^{(1)} + \lambda_2 D^{(2)} \dots, \lambda_n D^{(n)} = 0$ a linear combination of $D(i)$, $\lambda_i \in A$.

We have:

$$\begin{cases} \lambda_1 D^{(1)}(x_1) + \lambda_2 D^{(1)}(x_2) + \dots + \lambda_n D^{(1)}(x_n) = 0 \\ \lambda_1 D^{(2)}(x_1) + \lambda_2 D^{(2)}(x_2) + \dots + \lambda_n D^{(2)}(x_n) = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \lambda_1 D^{(n)}(x_1) + \lambda_2 D^{(n)}(x_2) + \dots + \lambda_n D^{(n)}(x_n) = 0 \end{cases}$$

where $\det(D^{(i)}(x_j)) = p^n u \neq 0$.

If $D^{(i)}(x_j) = pa_{ij}$, it follows:

$$\begin{cases} \lambda_1 a_{11} + \lambda_2 a_{12} + \ldots + \lambda_n a_{1n} = 0 \\ \lambda_1 a_{21} + \lambda_2 a_{22} + \ldots + \lambda_n a_{2n} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \lambda_1 a_{n1} + \lambda_2 a_{n2} + \ldots + \lambda_n a_{nn} = 0 \end{cases}$$

and $\det(D^{(i)}(x_j)) = p^n \det(a_{ij})$,

$$\det(a_{ij}) = u \in U(A).$$

Finally $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$.

Replacing $D^{(i)}$ by suitable linear combinations, we may assume that $D^{(i)}(x_j) = p\delta_{ij}$. When $r = 1$, the assertion is true by theorem 2. We can proceed by induction on r.

THEOREM 4. *Let (A, m) be a noetherian local ring, $k = Z_{pZ}$, and let $x_1, x_2, \ldots, x_r \in m$.*

Put $\Im = (x_1, x_2, \ldots, x_r)$.

Suppose that:

1) *p is not 0-divisor in A as well in $A/(x_1, x_2, \ldots, x_i)$, $1 \leq i \leq r$.*
2) *there exist $D^{(1)}, D^{(2)}, \ldots, D^{(r)} \in Der(A)$ $D_i : A \to pA$, $1 \leq i \leq r$ such that $[D_i, D_j] \in \Sigma pAD_i$ and*

$$\det(D^{(i)}(x_i)) = p^r u, u \in U(A).$$

Then the subring $F = \{a \in A/D_1(a) = \ldots = D_r(a) = 0\}$ is a coefficient ring of A mod $\Im$ in the sense that $A = F + \Im$, $F \cap \Im = (0)$.

Moreover we have $A = F[[x_1, x_2, \ldots, x_r]]$ with $x_1, x_2, \ldots, x_r$ analytically, independent over F and $\Sigma AD_i = \Sigma A(p\partial/\partial x_i)$, where $\dfrac{\partial}{\partial x_i}$ denotes the partial derivations in $F[[x_1, x_2, \ldots, x_r]]$.

Proof. We may replay the D_i by linear combinations of them and assume that $D_i x_j = p\delta_{ij}$, without destroying the integrability conditions $[D_i, D_j] \in \Sigma pAD_i$.

Now we prove that $A = F + \Im$.

Since the positive integers are non zero-divisor in A by assumption, the total ring of quotient, K of A contains Q.

Every derivation D of A can be extended to a derivation of K and since $\mathrm{char}(K) = 0$, D can be lifted to the iterarive differentiation $\underline{D} = \{1, D, D^2/2!, \ldots, D^n/n!, \ldots\}$ of K. If D maps A into pA, $D^n(A) \subseteq p^n A$, and it is possible to see that $D^n/n!$ maps A into A.

It follows that for any $y \in A$, we can define

$$y^{(1)} = y - \frac{1}{p}\sum_{i=1}^{n} D_i(y)x_i$$

$$\text{since} \quad \frac{1}{p}D_i(y) \in A, \quad \text{it follows that} \quad y^{(1)} \in A.$$

But $\dfrac{1}{p}D_i(D_i y) \in pA \subset A$, so we have

$$D_i y^{(1)} \equiv 0 \bmod (p\Im) \quad \text{and} \quad y^{(1)} \equiv y \bmod \Im.$$

By induction we can construct $y^{(1)}, y^{(2)}, \ldots \in A$ such that $y^{(k)} \equiv y^{(k-1)} \bmod \Im^k$ $D_i y^{(k)} \equiv 0 \bmod p^k \Im^k$, for $i = 1, 2, \ldots, r$ and for all positive integer k.

Suppose that we have constructed $y^{(1)}, y^{(2)}, \ldots, y^{(k)}$.

We can write

$$D_j y^{(k)} = p^k \sum_{1\le i_1 \le r} \cdots \sum_{1\le i_k\le r} b_{ij_1 \ldots i_k} x_{i_1} \ldots x_{i_k},$$

where we may suppose (by taking the arithmetic means over the distinct permutations of $i_1, \ldots, i_k$) that the coefficients $b_{ji_1 \ldots i_k}$ are symmetric in the indices $i_1, \ldots, i_k$. Now

$$D_h D_j y^{(k)} \equiv p^k \sum_{i_1} \cdots \sum_{i_k} \sum_{t=1}^{k} \delta_{hi_t} b_{ji_1 \ldots i_k} x_{i_1} \ldots x_{i_{t-1}} \ldots x_{i_k} \equiv$$
$$\equiv p^k \sum_{i_2} \cdots \sum_{i_k} k b_{jhi_2 \ldots i_k} x_{i_2} \ldots x_{i_k} \operatorname{mod} p^{k+1} \mathfrak{I}^k$$

and similarly

$$D_j D_h y^{(k)} \equiv p^{k+1} \sum_{i_2} \cdots \sum_{i_k} k b_{hji_2 \ldots i_k} x_{i_2} \ldots x_{i_k} \operatorname{mod} p^{k+1} \mathfrak{I}^k.$$

Since $[D_h, D_j]$ is a linear combination of the D_i's and since $D_i y^{(k)} \equiv 0 \operatorname{mod} p^k \mathfrak{I}^k$, we have $D_h D_j y^{(k)} \equiv D_j D_h y^{(k)} \operatorname{mod} p^{k+1} \mathfrak{I}^k$. By theorem 1 x_1 is not a 0-divisor of A, and $D_2, \ldots, D_r$ induce derivations of $A/x_1 A$.

Hence by induction we see that $x_1, x_2, \ldots, x_r$ is an A-regular sequence.

Therefore $gr^{\mathfrak{I}}(A) \cong (A/\mathfrak{I})[T_1, \ldots, T_r]$.

It follows from this and from the above congruences that

$$p^{k+1} \sum_{i_2} \cdots \sum_{i_k} k b_{jhi_2 \ldots i_k} x_{i_2} \ldots x_{i_k} \operatorname{mod} p^{k+1} \mathfrak{I}^k \equiv$$
$$\equiv p^{k+1} \sum_{i_2} \cdots \sum_{i_k} k b_{hji_2 \ldots i_k} x_{i_2} \ldots x_{i_k} \operatorname{mod} p^{k+1} \mathfrak{I}^k.$$

Since p is not 0-divisor and for $k \neq p$, k is invertible, it follows that

$$b_{hji_2 \ldots i_k} \equiv b_{hji_2 \ldots i_k} \operatorname{mod} \mathfrak{I}.$$

This means that $b_{i_1 \ldots i_{k+1}} \operatorname{mod} \mathfrak{I}$ is ymmetric in the $k+1$ indices.

Now define $y^{(k+1)}$ by

$$y^{(k+1)} = y^{(k)} - \frac{p^{k-1}}{(k+1)} \sum_{i_1=1}^{r} \cdots \sum_{i_{k+1}=1}^{r} b_{i_1 \ldots i_{k+1}} x_{i_1} \ldots x_{i_{k+1}}.$$

Then $y^{(k+1)} \equiv y^{(k)} \mathrm{mod} p^{k-1} \Im^{k+1}$, and

$$D_j y^{(k+1)} \equiv p^k \sum_{i_1 \dots i_k} b_{ji_1 \dots i_k} x_{i_1} \dots x_{i_k} - p^k \sum_{i_1 \dots i_k} b_{ji_1 \dots i_k} x_{i_1} \dots x_{i_k}$$

$$\equiv 0 \mathrm{mod} \Im^{k+1} \text{ since } y^{(k+1)} \equiv y^{(k)} \mathrm{mod} \Im^{k+1}.$$

Finally put $y_0 = \lim_{k \to \infty} y^{(k)}$ and get $y \equiv y_0 \mathrm{mod} \Im$ and $D_i y_0 = 0$ for all i, so that $y_0 \in \Im$ and $y \in F + \Im$.

The proof of the fact $F \cap \Im = (0)$ follows by Theorem 2.

THEOREM 5. *Let A be a noetherian k-algebra, $k = Z_{pZ}$ and let $I = (x_1, \dots, x_r) \subseteq m$. Suppose that:*

(1) p is not 0-divisor in A as well in $A/(x_1, \dots, x_i)$, $1 \le i \le r$.

(2) A is I-adically complete, and

(3) there exist iterative differentiations $\mathbf{D}^{(1)}, \dots, \mathbf{D}^{(r)}$ of A, $\mathbf{D}^{(i)} = \{1, D_1^{(i)}, D_2^{(i)}, \dots\}$, which commute with each other (i. e. $D_m^{(i)}$ and $D_n^{(j)}$ commute for any m, n i, j; when $i = j$ this follows from the iterativity), such that $D_1^{(i)} x_j = p\delta_{ij}$, $D_n^{(i)} x_j = 0$ $(n > 1)$.

Then we have the following facts:

i) the subring $F = \{a \in A / E^{(1)} a = \dots = E^{(r)} a = a\}$, where $E^{(i)}$ is the homomorphism $A \to A[[t]]$ corresponding to $\mathbf{D}^{(i)}$, is a coefficient ring of A mod I,

ii) $A = F[[x_1, \dots, x_r]]$ with $x_1, \dots, x_r$ analytically independent over F,

iii) for any formal power series $g(x_1, \dots, x_r)$ with coefficients in F we have $E^{(i)} g(x_1, \dots, x_r) = g(x_1, \dots, x_i + pt, \dots, x_r)$.

Proof. It suffices to prove $A = F + I$, because the rest of the proof is similar to that of Th. 3. We use in crucial manner the results contained in theorem 4 of [3].

Consider the ring homomorphism $E_{-x_i}^{(i)} : A \to A$ defined by

$$E_{-x_i}^{(i)}(y) = \sum_{n=0}^{\infty}(-x_i)^n D_n^{(i)}(y) \quad y \in A.$$

For any iterative differentiation $\mathbf{D} = \{D_0, D_1, D_2, \ldots\}$ and for any $x \in m$ such that $D_1 x = p$, $D_n x = 0$ $(n > 1)$, consider in the total ring of quotients of A, the differentiation

$$\mathbf{D}' = \{D_i'\} = \{D_0, D_1', D_2', \ldots\} = \left\{\frac{D_i}{p^i}\right\}.$$

It results

$$D_1'(x) = \frac{1}{p}D_1(x) = 1,\ D_n'(x) = \frac{1}{p^n}D_n(x) = 0.$$

$\mathbf{D}$ is an iterative differentiation and it results by theorem 4 of [3],

$$D_m'(E_{-x}(y)) = \frac{1}{p^m}D_m(E_{-x}(y)) = 0$$

$sD_m(E_{-x}(y)) = 0$, s non 0-divisor in A, hence $D_m(E_{-x}(y)) = 0$.

Therefore $E_{-x_i}^{(i)}(y)$ is a $\mathbf{D}^{(i)}$-constant.

It is easy to check that the homomorphisms $E_{-x_i}^{(i)}$, $1 \leq i \leq r$, commute with each other.

Therefore $E_{-x_1}^{(1)} E_{-x_2}^{(2)} \ldots E_{-x_r}^{(r)}(y) \in F$ for any $y \in A$ and this image is congruent to y modulo I. Hence $A = F + I$.

REFERENCES

[1] Matsumura H., *Integrable derivations,* Nagoya Math. J., **87** (1982), 227-245.

[2] Restuccia G., Matsumura H., *Integrable derivations in rings of unequal characteristic,* Nagoya Math. J., **93** (1984), 173-178.

[3] Restuccia G., Matsumura H., *Integrable derivations II,* Acc. Peloritana dei Pericolanti, **LXX**, (1992), 153-172.

Dipartimento di Matematica
Università di Messina